Microsoft Brokering File System Elevation of Privilege Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-26181
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 18:16:54 UTC
Updated	2026-04-23 18:19:28 UTC
Description	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from secure@microsoft.com

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000440000 probability, percentile 0.135890000 (date 2026-04-24)

Problem Types: CWE-362 | CWE-416 | CWE-416 CWE-416: Use After Free | CWE-362 CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 11 23h2	All	All	All	All
Operating System	Microsoft	Windows 11 23h2	All	All	All	All
Operating System	Microsoft	Windows 11 24h2	All	All	All	All
Operating System	Microsoft	Windows 11 24h2	All	All	All	All
Operating System	Microsoft	Windows 11 25h2	All	All	All	All
Operating System	Microsoft	Windows 11 25h2	All	All	All	All
Operating System	Microsoft	Windows 11 26h1	All	All	All	All
Operating System	Microsoft	Windows 11 26h1	All	All	All	All
Operating System	Microsoft	Windows Server 2022 23h2	All	All	All	All
Operating System	Microsoft	Windows Server 2025	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfo
CNA	Microsoft	Windows 11 Version 22H3	affected 10.0.22631.0 10.0.22631.6936 custom	ARM6
CNA	Microsoft	Windows 11 Version 23H2	affected 10.0.22631.0 10.0.22631.6936 custom	x64-b
CNA	Microsoft	Windows 11 Version 24H2	affected 10.0.26100.0 10.0.26100.8246 custom	ARM6
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.8246 custom	ARM6
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.1836 custom	ARM6
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.2274 custom	x64-b
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26181	secure@microsoft.com	msrc.microsoft.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**